

Secret Sharing

Henning Hontheim

10. März 2020

Inhaltsverzeichnis

1	Wozu Secret Sharing?	1
1.1	Ein kombinatorisches Beispiel	2
2	Primitives Secret Sharing	2
2.1	Aufsplitten des Secrets	2
2.2	One-Time-Padding	3
3	Shamir's Secret Sharing	3
3.1	$(2, n)$ -Schema	3
3.2	$(3, n)$ -Schema	4
3.3	Allgemeine (k, n) -Schemata	4
3.4	Shamir's Secret Sharing $x \bmod p$	4
4	Weitere Verfahren	4
4.1	Blakeley's	5
4.2	whatever...	5
5	Fazit	5
	Abbildungsverzeichnis	6
	Literaturverzeichnis	6

1 Wozu Secret Sharing?

In Public-Key-Infrastrukturen ist es oft nützlich, private Schlüssel von Teilnehmern rekonstruieren zu können. Aus Sicherheitsgründen ist es aber wichtig, dass nicht ein einzelner die Möglichkeit hat, geheime Schlüssel zu rekonstruieren. Eine Technik, um dieses Problem zu lösen, ist das Secret-Sharing, das in diesem Vortrag vorgestellt werden soll.

In Public-Key-Infrastrukturen ist es oft nützlich, private Schlüssel von Teilnehmern re- konstruieren zu können. Wenn nämlich ein Benutzer die Chipkarte mit seinem geheimen Schlüssel verliert, kann er seine verschlüsselt gespeicherten Daten nicht mehr entschlüsseln. Aus Sicherheitsgründen ist es

aber wichtig, dass nicht ein einzelner die Möglichkeit hat, geheime Schlüssel zu rekonstruieren. Es ist besser, wenn bei der Rekonstruktion von privaten Schlüsseln mehrere Personen zusammenarbeiten müssen. Die können sich dann gegenseitig kontrollieren. Die Wahrscheinlichkeit sinkt, dass Unberechtigte Zugang zu geheimen Schlüsseln bekommen. In diesem Kapitel wird eine Technik vorgestellt, dieses Problem zu lösen, das Secret-Sharing. [1] [3]

1.1 Ein kombinatorisches Beispiel

Mehrere Wissenschaftler N arbeiten zusammen an einem Geheimprojekt. Um die Dokumente geheim zu halten und um Missbrauch vorzubeugen, verschließen sie diese in einem Tresor. Nur wenn mindestens die Hälfte aller Wissenschaftler anwesend ist, soll sich der Tresor öffnen lassen. Wie viele paarweise verschiedene Schlösser S muss der Tresor mindestens besitzen? Wie viele paarweise verschiedene Schlüssel s muss jeder Wissenschaftler mindestens bei sich tragen? Siehe [3] nach [2].

Beispiel 1.1. Sei $N = 11$ die Anzahl aller Wissenschaftler und $n = \lceil \frac{N}{2} \rceil = 6$ die Anzahl derer, die mindestens anwesend sein müssen, damit sich der Tresor öffnen lässt. Folglich muss es also für jede Teilmenge mit k Wissenschaftlern, wobei $k = N - n = 5$, genau ein Schloss geben, für das keiner der k Wissenschaftler einen Schlüssel besitzt. Also muss der Tresor $S = \binom{N}{k} = \binom{11}{5} = 462$ paarweise verschiedene Schlösser besitzen.

Sei $W = \{w_1, w_2, \dots, w_k, w_{k+1}\}$ mit $|W| = k + 1 = 6$ die Menge von Wissenschaftlern, die mindestens benötigt wird, um den Tresor zu öffnen. Dann gibt es genau ein bestimmtes Schloss S' , für das keiner der Wissenschaftler aus $W \setminus w_{k+1}$ einen Schlüssel besitzt, der Wissenschaftler w_{k+1} jedoch schon. Da für jede Permutation von $k = 5$ Wissenschaftlern genau der w_{k+1} existiert, der die Teilmenge W „vervollständigt“, bekommt jeder Wissenschaftler $s = \binom{N-1}{|W|-1} = \binom{N-1}{k} = \binom{10}{5} = 252$ Schlüssel. Das ergibt eine Gesamtanzahl an $11 \cdot 252 = 2772$ Schlüsseln. Dass dies keine praktikable Lösung des Problems ist, ist offensichtlich.

2 Primitives Secret Sharing

2.1 Aufsplitten des Secrets

Blah

Beispiel 2.1. Zahl aufteilen

2.2 One-Time-Padding

Blah

Beispiel 2.2. Zwei Personen

Beispiel 2.3. n Personen

Beispiel 2.4. Visuelles Beispiel

3 Shamir's Secret Sharing

Blah

3.1 $(2, n)$ -Schema

Blah

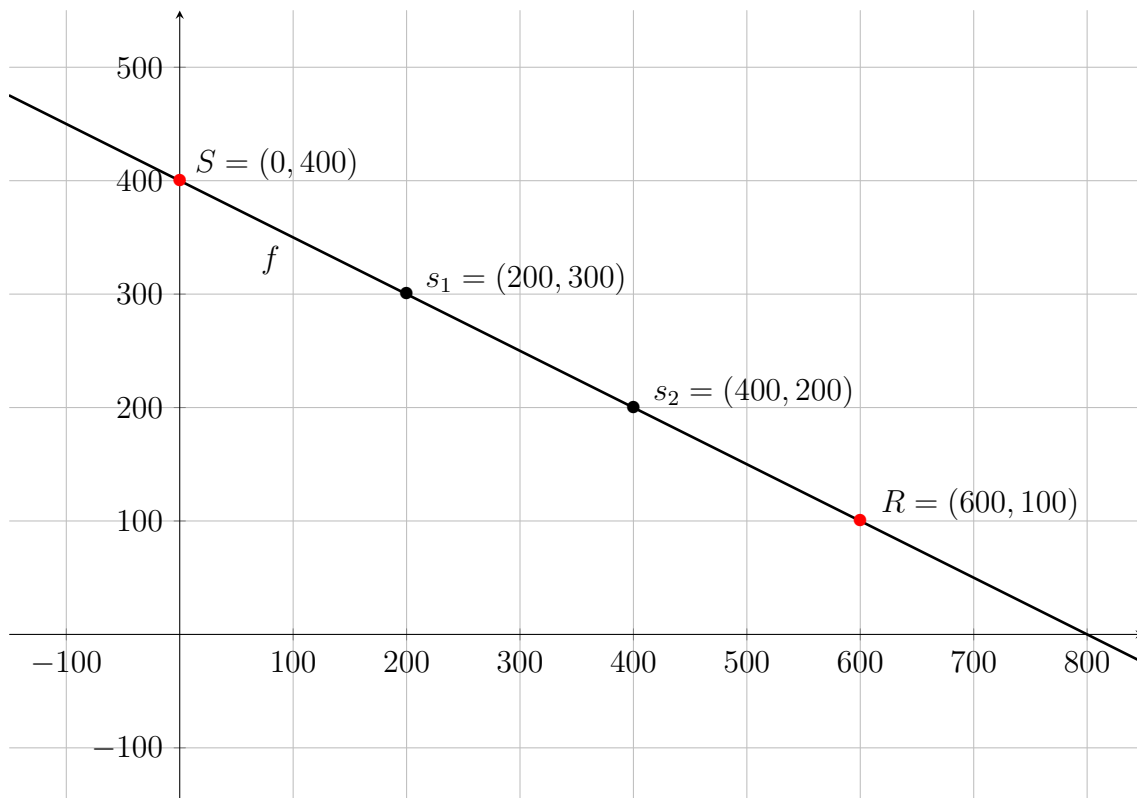


Abbildung 1: Erweiterung des Geheimnisses S als Gerade f für zwei Shares s_1 und s_2 .

3.2 $(3, n)$ -Schema

Blah

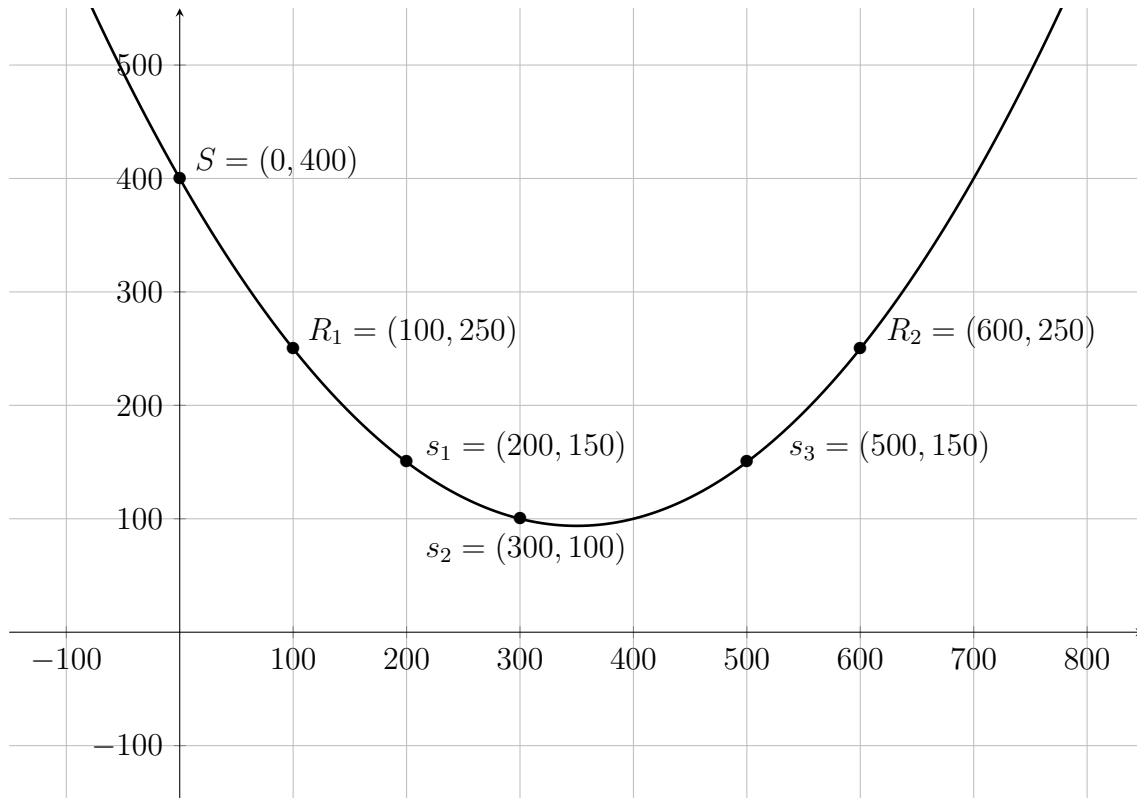


Abbildung 2: Parabel

3.3 Allgemeine (k, n) -Schemata

Blah

3.4 Shamir's Secret Sharing $x \bmod p$

Blah

4 Weitere Verfahren

Blah

4.1 Blakeley's

Blah

4.2 whatever...

Blah

5 Fazit

Abbildungsverzeichnis

1	Erweiterung des Geheimnisses S als Gerade f für zwei Shares s_1 und s_2	3
2	Parabel	4

Literaturverzeichnis

- [1] BUCHMANN, J. *Einführung in die Kryptographie*. Springer Berlin Heidelberg, 2016.
- [2] LIU, C. L. *Introduction to Combinatorial Mathematics*. McGraw-Hill, New York, 1968.
- [3] SHAMIR, A. How to share a secret. *Communications of the ACM* 22, 11 (Nov 1979), 612–613.